eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Tipos de Varreduras**
  - ✓ Varreduras Passivas
  - ✓ Varreduras Ativas
  - ✓ Varreduras Furtivas
  - ✓ Varreduras Passivas: Google Hacking
    - ✓ Conceito
    - ✓ Exemplos de uso
    - ✓ Operadores
    - ✓ Colocando em Prática

Varreduras

Há 3 tipos de varreduras que podemos utilizar em nosso ambiente para detectar possíveis ataques.

1. **Varreduras Passivas**

   As varreduras Passivas, buscam outros métodos de coletar dados do alvo, sendo assim, tornando-se indetectáveis, porém, não tão específicas como as varreduras Ativas
2. **Varreduras Ativas**

   Quando realizamos varreduras Ativas, vamos direto ao alvo, com o objetivo de coletar dados precisos sobre o ambiente atual. Essa técnica é de fácil detecção por Firewalls/IDS/WAFs e afins.
3. **Varreduras Furtivas**

   Varreduras Furtivas tem o objetivo de utilizar as técnicas das varreduras Ativas, porém, com a menor probabilidade de detecção. Efetuando evasões de sistemas de detecção e confundindo os administradores de uma rede.

Google Hacking – Varredura Passiva

Google Hacking: Entendendo

O Google hacking envolve o uso de operadores avançados no Google, motor de busca para localizar sequências específicas de texto dentro de resultados de pesquisa. Alguns dos exemplos mais populares são, encontrar versões específicas de grupos vulneráveis em aplicações web.

Alguns dos exemplos mais populares é encontrar versões específicas de grupos vulneráveis em aplicações web. As consultas de pesquisas a seguir seriam localizar todas as páginas que possuem um determinado texto contidas na página.

Através do Google Hacking, você pode encontrar particularidades que talvez já tenham até saído do ar. Obtendo um número razoável de informações sobre um determinado alvo, é possível explorar suas vulnerabilidades.

Esta ferramenta é tão robusta que pouco conhecemos sobre ela, primeiramente, devemos entender como o google funciona:

Google Hacking

Exemplos:
"site:" - faz uma busca dentro de um dominio.
Ex.: "big brother site:globo.com"
Vai listar todas as paginas no dominio globo.com que contem "big brother".

"allintitle:" - faz uma busca por paginas que contem palavras especificas no titulo.
Ex.: "allintitle:seja bem vindo"
Busca todas as paginas com titulo contendo as seguintes palavras "seja bem vindo".

"allinurl:" - faz uma busca por endereços de url que contem palavras especificas.
Ex.: "allinurl:contato.asp"
Busca todos os sites contendo "contato.asp" na url.

"inurl:" – Busca determinadas palavras dentro de um domínio
Ex.: senhas "inurl:esecurity.com.br"
Irá efetuar uma busca da palavra senha no dominio esecurity.com.br

Google Hacking

Exemplos:
“filetype:“ - faz uma busca em determinadas extensões de arquivos.
Ex.: “senhas filetype:txt"
Irá buscar todos os arquivos .txt que possui palavras senhas dentro dele.

"allinurl:" - faz uma busca por endereços de url que contem palavras especificas.
Ex.: "allinurl:contato.asp“
Busca todos os sites contendo "contato.asp" na url.

“inurl:” – Busca determinadas palavras dentro de um domínio
Ex.: senhas “inurl:esecurity.com.br”
Irá efetuar uma busca da palavra senha no dominio esecurity.com.br

Google Hacking

Operadores:
"-" – Remove palavras ou dados que não devem ser apresentados
Ex.: "justin -bieber"
Irá buscar todas as páginas que possuem algo relacionado a qualquer Justin, desde que não possua nenhuma palavra que remete à Bieber, no caso, Justin Bieber não deve aparecer (Graças a Deus)

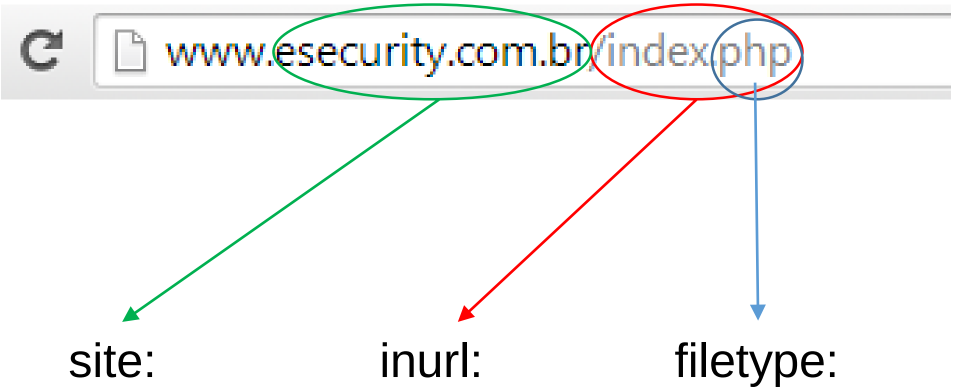
"+" – Força o aparecimento de palavras ou dados que devem ser apresentados.
Ex.: "academia +hacker"
Irá efetuar a busca em todos os sites que possui a palavra academia onde na mesma página também encontra-se a palavra hacker.

"OR" – Dados booleanos, você pode optar por aparecer um ou outro. Também pode substituir o OR por |
Ex.: Vodka OR Água de Côco
Irá efetuar uma busca da palavra Vodka ou a frase Água de côco

Google Hacking

“AND” – Você pode optar por buscar por 2 ou mais dados simultâneos.
Ex.: Alan AND Sanches AND Security
Irá efetuar uma busca da palavra Alan Sanches e Security, caso a página não tenha essas 3 informações, não será listada.

Google Hacking



Google Hacking

Exemplos de uso como ferramenta hacking:

"allinurl:usuarios.mdb site:.com.br"
Busca por arquivos de banco de dados nomeados "usuarios.mdb" dentro do dominio mae ".com.br"

"allintitle:admin panel site:.org"
Busca por supostas paginas de administracao dentro do dominio ".org"

"allinurl:login.asp"
Lista todas as paginas com nome de "login.asp", e em alguns casos o google exibira uma versão "cache" da pagina onde será possível ver o codigo asp.

Google Hacking: Roubando senhas

Buscando arquivos de anotações de senha:

 # intitle:"index of /" senhas.txt

 # inurl:admin intext:username= AND email= AND password OR pass=

filetype:xls + senha + com.br

filetype:txt intext:senha

Alvo interessante: http://static.tumblr.com/eeczvca/Bi9m1gu4l/my_senhas.txt

Invadindo PhpMyAdmin sem senha

 # inurl:"phpmyadmin/index.php" intext:"[Edit] [Create PHP Code] [Refresh]"

Google Hacking: Juice Files Info

Buscando backup de configurações de CMSs

 # intext:"~~Joomla1.txt" title:"Index of /"
Alvo interessante: http://tiagofeitosa.com/cb/

 # configuration.php_ “<?php class Jconfig {“

 # inurl:wp-config.old
#inurl:"configuration.php.old" class JConfig

inurl:configuration.php.bkp
Alvo interessante: http://www.philippinedirect.com/configuration.php.bkp

Google Hacking: Impressoras remotas

Invadindo impressora remota

 # intitle:”Web Image Monitor” & inurl:”/mainframe.cgi”

Google Hacking: Controlando câmeras

Buscando câmeras disponíveis na internet:

 # inurl:LvAppl intitle:liveapplet

 # intitle:"Live View - AXIS 211"

 # inurl:"viewerframe?mode=motion“

 # inurl:”/control/userimage.html”

Google Hacking: Arquivos importantes

Buscando por arquivos de VPN

 # !HOST=.* intext:enc_UserPassword=* ext:pcf*

Google Hacking: Brinde!

Seguem lista de dorks mais comuns e suas respectivas falhas:

Lista de Dorks para ataques XSS:
 # http://www.esecurity.com.br/blackhat2/dorks/dorks-xss.txt

Lista de Dorks para ataques LFI:
 # http://www.esecurity.com.br/blackhat2/dorks/dorks-lfi.txt

Lista de Dorks para ataques RFI:
 # http://www.esecurity.com.br/blackhat2/dorks/dorks-rfi.txt

Lista de Dorks para ataques SQL:
 # http://www.esecurity.com.br/blackhat2/dorks/dorks-sql.txt

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker